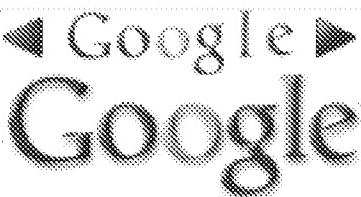


[Web](#) [Images](#) [Maps](#) [News](#) [Shopping](#) [Gmail](#) [more ▾](#)

[Sign in](#)

VMM TPM

Search

[Advanced Search](#)
[Preferences](#)


Web

Results 1 - 10 of about 17,100 for **VMM TPM**. (0.20 seconds)

1. Security architecture of trusted virtual machine monitor for ...

secrecy of a closed-box VM is protected by **VMM**. **TPM**. is used to attest the VM running critical application and. TVMM to remote party.

www.springerlink.com/index/J5363Q744174G2M4.pdf - [Similar pages](#)

by Q Huang - 2007 - [Related articles](#)

2. Sharing trusted hardware across multiple operational environments ...

VMM TPM Multiplexer 108 is a thin layer of software between the VMs and the **TPM** ...

VMM TPM Multiplexer 108 maintains virtual hash values corresponding to a ...

www.freepatentsonline.com/y2005/0210467.html - [Similar pages](#)

by VJ Zimmer - 2004

3. [PPT] **TPM**-Performance Sensible Key Management Protocols for Service ...

File Format: Microsoft Powerpoint - [View as HTML](#)

while the measurement of the **VMM** is infrequent and reasonably performed by the low-performance **TPM**, the delegated attestation and storage protection are ...

www.daoliproject.org/twiki/pub/Daoli/Slides/16th_SPW.ppt - [Similar pages](#)

4. **VMM** Headlines TechNet Magazine

Feb 19, 2008 ... **VMM** Headlines TechNet Magazine ... and prompted readers to explore the 4000+ word overview of **VMM** 2007 by **VMM**'s own **TPM** Edwin Yuen.

www.ditti.com/2008/02/19/vmm-headlines-technet-magazine/ - [Similar pages](#)

5. Re: **TPM** & disk crypto

Both technologies relied on the **TPM** chip to take measurements of running ... the **TPM**) and launch a hypervisor, that is, a Virtual Machine Monitor (**VMM**).

www.mail-archive.com/cryptography@metzdowd.com/msg06831.html - 17k

- [Cached](#) - [Similar pages](#)

6. Background

... background on the two technologies that are basic to understanding this paper: the Trusted Platform Module (**TPM**) and the Virtual Machine Monitor (**VMM**).

www.usenix.org/events/sec06/tech/full_papers/berger/berger_html/node2.html - 9k

- [Cached](#) - [Similar pages](#)

by S Coprocessing - 2005 - [Related articles](#) - [All 2 versions](#)

7. [PDF] The Intel Safer Computing Initiative

File Format: PDF/Adobe Acrobat - View as HTML

Obtaining the VMM Identity 94. SMX Measurement Instructions 95. Chipset Hardware

96. Storing VMM Measurement in TPM 96. Other CPU Resources 97 ..

support.intel.com/intelpress/toc-secc.pdf - Similar pages

by D Grawrock - Cited by 40 - Related articles - All 6 versions

8. Platform configuration register virtualization apparatus, systems ..

[0009] The apparatus 100 may include a **TPM** 114 and a virtual machine monitor.

(VMM) 116 coupled to the TPM 114 to virtualize the TPM resources 111. . .

www.freshpatents.com/Platform-configuration-register-virtualization-apparatus-systems-and-methods-dt20061012ptan2... - 32k - [Cached](#) - [Similar pages](#)

9. [PDF] Microsoft PowerPoint - AFEI Software Assurance Conf.ppt

File Format: PDF/Adobe Acrobat - View as HTML

VMM during launch process. • Process to ensure proper reporting and storage of

VMM measurement in TPM. • All processors participate. DMA protection ...

www.afei.org/brochure/6a08/documents/AFEI_Software_Assurance_Richmann.pdf
- Similar pages

10. [PDF] TPM-Performance Sensible Key Management Protocols for Service ..

File Format: PDF/Adobe Acrobat - [View as HTML](#)

software component: virtual machine monitor (**VMM**). A measured **VMM** is denoted MVMM, which is considered an extension of the **TPM** as a trusted computing base ..

spw.feis.herts.ac.uk/Pre-Proceedings/09-Mao-SPWv9.pdf - Similar pages

1 2 3 4 5 6 7 8 9 10 [Next](#)

VMM TPM

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#) | [Try Google Experimental](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [Privacy](#) - [About Google](#)